楕円曲線の計算にみる数論システムの進展状況 (数式処理 : その研究と目指すもの)

AUTHOR(S):

横山, 俊一

CITATION:

横山, 俊一. 楕円曲線の計算にみる数論システムの進展状況 (数式処理 : その研究と目指すもの). 数理解析研究所講究録 2012, 1785: 57-66

ISSUE DATE:

2012-03

URL:

http://hdl.handle.net/2433/172739

数理解析研究所講究録
第1785巻 2012年 57-66

楕円曲線の計算にみる数論システムの進展状況

九州大学大学院数理学府D2　横山 俊一（Shun'ichi Yokoyama）
Graduate School of Mathematics, Kyushu University

概要　近年の計算機環境の進歩は目覚ましく，数年前では不可能と考えられていた計算も容易になりつつある．この背景には，スーパーコンピュータ等のプロセッサ・ハードウェアの開発技術の向上もさることながら，個人計算機として使用出来るPCのスペック向上・計算機代数ソフトウェアの機能充実も大きな要因として挙げられる．そこで本稿では，現代数論の研究における最重要対象の一つである楕円曲線を取り上げ，どのような計算が可能となっているのか，昔は出来なかったが今は可能となった計算にはどのようなものがあるのか，そして今後どのような事を計算したいと願っているかについて，非専門家向けに報告を行う．なお本稿の内容は，著者が2011年12月8日（木）に本集会にて行った講演内容に沿っている．

1　数論ソフトウェアと楕円曲線の研究

楕円曲線（elliptic curve）とは，

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$$

という形の方程式（Weierstrass方程式と呼ぶ）で定義される非特異3次曲線のことである[1]．現代数論において，この曲線は非常に多くの応用と重要な話題を提供することから，数多くの研究者が考察を重ねている．近年の楕円曲線暗号への貢献や，楕円曲線の理論の一般化であるアーベル多様体の理論の進展などは目覚ましく，これだけ簡易に定義出来る数学的対象の大きな神秘を感じることが出来る．

さて，上記の楕円曲線は「どの体上で考えるか」によってその様相が大きく異なる．例えば有限体 $\mathbb{F}_p$（p は有理素数）上や位数 p 冪の体 $\mathbb{F}_{p^n}$ 上の楕円曲線が楕円曲線暗号の研究に用いられる．一方，数論的興味として高次元化（代数曲面としてとらえる方法）を考える際には複素数体 $\mathbb{C}$ 上で考えることが多い．特に楕円曲線を考察する上では，有理点（rational point）の構造を調べることが非常に大切なのであるが，その構造は基礎体の違いで大きく変わってしまう．簡単な例として

$$E:\ y^2=x^3+1728$$

という形の曲線を考えよう．楕円曲線の著しい性質として，どのような基礎体上であっても有理点全体の集合は群構造を持つことが知られており，**Mordell-Weil群**[2]と呼ばれている．先の曲線を有理数体 $\mathbb{Q}$ 上の曲線と見做せば，Mordell-Weil群 $E(\mathbb{Q})$ は位数2の巡回群 C_2 に同型であり，E 上の点 $(-12,0)$ で生成される．ところが基礎体を二次体 $\mathbb{Q}(\sqrt{43})$ に取りかえると，Mordell-Weil群 $E(\mathbb{Q}(\sqrt{43}))$ は $\mathbb{Z}\oplus C_2$ に同

[1]実はWeierstrass型でない楕円曲線というものもあり，本来は種数1の非特異射影曲線（に少しの制約がついたもの）のことである．本稿では簡単のためこのケースは扱わないこととする．

[2]「モーデル・ヴェイユ」と読む．Louis J. Mordell (1888-1972) と André Weil (1906-1998) の2名の数学者．

型であり, 自由部分が出現する. 因みに捩れ部分の生成元は先と同じで, 自由部分の生成元は $\left(-\frac{104}{9}, -\frac{56}{27}\sqrt{43}\right)$ である. Mordell-Weil 群の構造の変化は, 基礎体の変化からは全く予想のつかない振る舞いを見せることが多い.

以降, 本稿では主に一般の代数体（つまり標数 0 の体）上の楕円曲線の計算, 特にその場合の Mordell-Weil 群の計算について考える. $\mathbb{Q}$ の場合もこれに含まれるが, 最近のソフトウェアの改善に伴ってかなりの計算が高速に出来るようになってきた. その一方で, 代数体上の楕円曲線の計算は例え基礎体が二次体であっても十分困難な状況が続いている.

さて本論の前に, 近年の数論ソフトウェアの現状について少しだけ述べておくことにする. 良く知られている数論システムをざっと書き出してみると, 大体以下のようなものが思い浮かぶであろう：

> SIMATH, KANT-KASH (TECC-KASH), Pari/GP, Risa/Asir, Maple,
> MAGMA, Mathematica, NZMATH, Sage, $\cdots$

どれも数論システムとしては非常に多くの機能を備えており, また個人で所有する PC でも動くという面で非常に使い勝手が良い. 最初の SIMATH は既に開発が終了してしまっているが, その開発権そのものは首都大学東京に譲渡されたとの情報がある. なお, 首都大のチームが初の国産数論システムとして現在開発を進めているものが NZMATH であり, 楕円曲線絡みでは暗号系の研究に使用する目的から, 現在は有限体上のもののみ実装が行われている状態のようである. これと最後の Sage は, 開発言語として C ではなく Python を使用している. 国産のシステムとしてはもう一つ Risa/Asir が挙げられ, これは神戸大学・富士通研究所によって開発されている. Maple と MAGMA は有料, それ以外は（各種ライセンスは異なるが）無料で使用出来るようになっている.

正直な感想を述べると, 今回のように代数体上の楕円曲線を計算する上でどのインターフェースを用いるのが最適なのかは未だ分からない. 現時点では筆者は Pari/GP と MAGMA の組み込み関数を使い, Sage で統合環境を用意してプログラムを組んでいるが, これは要するに「Pari/GP と MAGMA の良い所取り」である. 例えば楕円曲線の不変量の一つとして導手（conductor）があるが, これを計算するためには Tate のアルゴリズムと呼ばれるものを用いる. 1990 年代後半に初めて実装手順を記した論文が発表され, その後幾つかの数論システムに搭載されたが, その中で最も高速かつ信頼性の高い MAGMA を使っている, という位の気持ちである. 従って別のアルゴリズムで Pari/GP の実装の方が早いものはそちらを採用しており, 将来第 3 の最も高速な実装が見つかった場合はそちらに乗り換える可能性も十分あり得る.

2 種々の楕円曲線の計算

現時点では特に $\mathbb{Q}$ 上および $\mathbb{F}_p$ 上の場合はかなりの計算が可能となっている. これについて幾つか具体的な事例を使って説明しよう. まずは主に $\mathbb{Q}$ 上の場合から始める：

- **不変量（invariant）**　導手（conductor）や玉河数（Tamagawa number）などが挙げられる．これらは3章で扱う代数体上の楕円曲線でも計算可能である．例えば導手は楕円曲線の還元の様子を如実に表す量であり，悪い還元（bad reduction）を持つような素点が因子として出現する．逆に言えば，もしも楕円曲線が至る所良い還元を持つならば，導手は自明となる[3]．逆に，与えられた導手を持つような楕円曲線のリストを計算する営みも行われている．John Cremona（Warwick大学）よるデータベースは，2011年12月9日現在で210,000以下の導手について公開されている．なお，楕円曲線の考察には他に判別式（**discriminant**）が使用されることが多い．但しこの量は楕円曲線のモデルの取り方に依存する[4]ため，導手等とは異なり不変量とはなりえない．

- **Mordell-Weil 群（Mordell-Weil group）**　1章でも述べた通り，有理点（この場合は各成分が有理数）全体のなす群を求める．$\mathbb{Q}$ 上の場合には数多くの実装が存在しており，例えば Cremona による `mwrank` などが有名である．

- **L-関数（L-function）**　通常の L-関数に加えて p 進版も扱えるようになってきた．L-関数は解析的に定義されるため，計算機上では高速に処理出来ることが多い．例えば有名な未解決予想であるバーチ・スウィンナートン-ダイアー予想（**BSD 予想**）は，代数的構造物である Mordell-Weil 群の階数が，解析的構造物である L-関数から導かれることを主張しており，計算機を用いて予想されたものである．実際，この予想が成り立つと仮定して「推定階数」を求める関数も幾つかのシステムに実装されている．

- **シャファレヴィッチ・テイト群（Shafarevich-Tate group）**　この群に関しては3章で紹介する．構造を理解することが非常に困難な群として知られており，計算機上での実現も同様である．この 2-torsion part を可視化するという方面の研究も見受けられる．

- **ヒーグナー点（Heegner point）**　ここでは詳細は割愛する．応用例として例えば Mordell-Weil 群の階数が1で，かつその free-part の生成元の求解が非常に困難な場合，この点を求めることで比較的容易に求められることがある[5]．特に数論幾何の方面でよく観察されており，p 進 Gross-Zagier 公式などはこれを使って記述される．

- 他にも **同種写像とその類（isogeny map / class）**，**同型写像（isomorphism）の構成** などはかなり容易に求めることが出来る．

---

[3]実は $\mathbb{Q}$ 上では Tate によって至る所良い還元を持つような楕円曲線が存在しないことが示されている．代数体上ではそのような例が存在し，このとき導手が自明であるとは，導手が自明なイデアル (1) となることである．

[4]但しある条件を満たすような代数体上であれば，**大域極小モデル（global minimal model）**の存在が保証されている．このモデルに限れば，最小の判別式は unique に定まる．

[5]この手法は Mordell-Weil 群の階数が2以上の場合には適用出来ない．その場合は，より高次の algebraic descent を用いて**超楕円曲線（hyperelliptic curve）**へ持ち上げる手法等で代用する．本稿では詳細は省かせて頂く．

また, 有限体 $\mathbb{F}_p$ 上の場合は特有の機能が見受けられる：

- **素因数分解アルゴリズム（ECM）**　特に暗号論では重要な意味を持つ, 有理整数の素因数分解アルゴリズムに楕円曲線を援用して高速化を図ったものである. どのようなアルゴリズムが実装されているかはシステムによって多少異なる. 例えば Sage には Zimmermann らによるアルゴリズム GMP-ECM が搭載されており, 比較的高速と評判が良いようである. 試しに

$$n = 22397447422083597502024595718624709634477861696504215$$
$$60804978144723333977920476664877327716487683639603$$

を素因数分解すると

$$p_1 = 1099511627791$$
$$p_2 = 20370359763344860862684456884093781610514683936659362506361404493543812997633367061833975333$$

と分解されるが, これを Pari/GP の組み込み関数を用いて行うと約4秒（CPU time）を要したのに対し, GMP-ECM では約0.2秒（CPU time）で終了した.

- **ペアリング（pairing）**　近年の楕円曲線暗号では良く知られている「ペアリング暗号」に関する実装も幾つか登場している. 例えば幾つかのシステムでは標準で Weil ペアリングが扱えるようになっている. 他に Tate ペアリングもよく用いられている.

3　代数体上の楕円曲線における algebraic descent

まず先述の Mordell-Weil による定理を載せておく.

定理 3.1 (Mordell-Weil). K を代数体, E を K 上定義された楕円曲線とする. E 上の K-有理点[6]のなす群 $E(K)$ は有限生成アーベル群である.

従って有限生成アーベル群の基本定理から, $E(K)$ は一意的に

$$E(K) \simeq \mathbb{Z}^{\oplus n} \oplus G$$

という形で書ける（ここに G は有限群）. この構造を決定することが今回の大きな目標である. ここでは最も一般的な手法を紹介する：

[6]ここでは「x 座標, y 座標どちらも K の元となる E 上の点」と解釈して頂いて差し支えない.

アルゴリズム **3.2** (**2-descent** 法). $E(K)$ は次の2ステップにより計算出来る.

1. 次の完全系列を用いて, $E(K)/2E(K)$ の生成元を求める (2-descent part):

$$1 \longrightarrow E(K)/2E(K) \longrightarrow \mathrm{Sel}^{(2)}(E/K) \longrightarrow Ш(E/K)[2] \longrightarrow 1$$

2. $E(K)/2E(K)$ から $E(K)$ を復元する (infinite descent part).

まず 2-descent part を解説する. 完全系列の中央にあるのは 2-Selmer 群と呼ばれるものであり, 数論においては非常に重要な群として認識されている. この群を計算することにより, その情報から $E(K)/2E(K)$ の構造を決定するという方法である. ここで問題となるのは, 右側にある群 $Ш(E/K)[2]$ であり, これは Shafarevich-Tate 群 (の 2-torsion) と呼ばれている. 本体 $Ш(E/K)$ はガロアコホモロジーの言葉で

$$\bigcap_v \mathrm{Ker}\left(H^1(G_K, E) \to H^1(G_{K_v}, E_v)\right)$$

と定義される群[7]であるが, この構造を求めることは非常に難しく, 実際この 2-torsion part だけであっても一般の計算アルゴリズムは知られていない. 従って, この群が本質的に寄与しない, 即ち trivial な場合は計算が成功することがあるが, non-trivial な場合は殆どこのアルゴリズムは成功しない.

続いて infinite descent part に移る. $h(P)$, $\hat{h}(P)$ を, それぞれ $P \in E$ の absolute logarithmic height, canonical height とする. まず実数 B を, 集合

$$\left\{P \in E(K) \mid \hat{h}(P) \leq B\right\}$$

が $E(K)/2E(K)$ の完全代表系を含むようにとると, この集合は $E(K)$ を生成することが Cremona [1] によって示されている. 更に Silverman [3], Siksek [2] によって, 任意の $P \in E(K)$ に対し

$$h(P) - \hat{h}(P) \leq B'$$

を満たす B' が存在することが知られている. この2つの事実より, $E(K)$ の生成元は必ず $h(P) \leq B + B'$ を満たしているので, この範囲で P を全て探索し, 逐次 $E(K)$ を構成していけば良い.

しかしながら, この手法は後半の全探索にかなりの時間を要する. 実際, 探索すべき点の個数は指数関数的に増加して行くことが分かっている. また, 有理数体上で特有の効率的な手法が適用出来ないケースも多々ある. このため, 例え基礎体の拡大次数が2や3程度であってもかなりの確率で計算が失敗してしまうことがある.

それでは, 代数体上の楕円曲線の 2-descent の実装例を2つだけ紹介しておく.

- **`TwoSelmerGroup` and `PseudoMordellWeilGroup` on MAGMA** MAGMA には, Mordell-Weil 群を計算するコマンドは搭載されていないが, 先程述べた 2-Selmer 群を計算する関数, そして Mordell-Weil 群の奇数指数部分群を探す `PseudoMordellWeilGroup` という関数が用意されている. 計算のための bound も調整出来るようになっているが, 調整可能なパラメータは1種類だけである.

[7]本論から外れるため本稿では記号の詳しい説明は割愛させて頂く.

- **Simon's 2-descent / Bruin's 2-descent**　何れも上述の 2-descent を実装したものであるが, 作成者独自の機能が追加されている. 例えば Simon's 2-descent に関しては, 2-Selmer 群を計算する途中で考察しなければならない Diophantus 方程式の簡略化（或る種のノルム方程式へ帰着）をベースに, 高速化が図られている（原論文 [4] 参照）. また, 調整可能なパラメータも数種類用意されている. また, 実装インターフェースも異なり, Simon のそれは Pari/GP, Bruin のそれは KASH で実装されている. 後者は Magma へのインプリメントもほぼ完了しているようである（作者からは prototype というアナウンスのままである）. なお Simon の Pari/GP コードの最新版は 2011 年 4 月版であり, それ以前のバージョンにはバグが存在している[8]. このバージョンの Simon's 2-descent は, Sage における組み込み関数 `simon-two-descent` に使用されているため, Sage のバージョンアップには反映されていないので注意が必要である[9].

4　具体例

唐突であるが, 次のような楕円曲線を考える：

$$y^2 + \sqrt[3]{46}xy + \frac{\sqrt[3]{46^2} + \sqrt[3]{46} + 1}{3}y$$
$$= x^3 + (\sqrt[3]{46} + 1)x^2 + \frac{C_1\sqrt[3]{46^2} + C_2\sqrt[3]{46} + C_3}{3}x + \frac{C_4\sqrt[3]{46^2} + C_5\sqrt[3]{46} + C_6}{3}$$

ここに C_k $(1 \leq k \leq 6)$ は次で与えられる.

$$\begin{aligned}
C_1 &= 942195937574333906814938647 06, \\
C_2 &= 108133470918663218473194761 7604, \\
C_3 &= 508408703554383043712880855 0119, \\
C_4 &= 232584233344792957094732754749860256404578 67, \\
C_5 &= 827892116462926667504946133778759990377913857, \\
C_6 &= 326497412111533344905526205920140161442668 6175.
\end{aligned}$$

この曲線は $\mathbb{Q}(\sqrt[3]{46})$ 上至る所良い還元を持つ楕円曲線のひとつの例である. この時, 本当にこの曲線が至る所良い還元を持つかどうかを確かめる為には

[8]木村巌氏（富山大学）との personal discussion から見つかったものである. 2011 年 4 月の Simon 氏自身による最新版へのアップデートは, このバグの除去によるものである.

[9]Sage のバグトラッキングシステムには報告済み. `6:28:14 pm, January 4th, 2011` 付けの Sage-Support に投稿されており, ログも残されている. ここでは $\mathbb{Q}(\sqrt{43})$ 上の楕円曲線 $y^2 = x^3 + 1728\varepsilon$ (ε は基本単数) の Mordell-Weil 群の計算が失敗するという件であった. 因みに同一の形の楕円曲線は $\mathbb{Q}(\sqrt{41})$ 上では計算出来る. バグの発生個所では `...iv,r=nfsqrt(nf,norm(zc))[1];if(DEBUGLEVEL-ell)` というコマンドラインでのデバッグエラーが報告された.

- 判別式 $\Delta(E)$ が $\pm\varepsilon^n$ の形で書ける.
- 導手 $N(E)$ が自明, 即ち 1 で生成されるイデアル (1) である.

の何れかが示せれば良い（但し ε は基礎体の基本単数）. 実際, 一つ目については計算してみると

$$\begin{aligned}\Delta(E) &= -37939843977345817008905171961789129388050638797011096888590698412408721460014652084422369603\sqrt[3]{46^2}\\ &\quad +38266373510239702375947834653456075318013469606118717466402223327610129260665089286586642440\sqrt[3]{46}\\ &\quad -88402196060375965791126700381485837764341711498964900463229074317241483287536740383170905601\\ &= -\varepsilon^{24}\end{aligned}$$

となっていることが分かる（ここに $\varepsilon = 309\sqrt[3]{46^2} + 48\sqrt[3]{46} - 4139$）. しかしながら, 最後の等式を片っ端から確かめるわけにはいかないので, 大抵の場合は二つ目の導手の計算を行う. そこでは 1 章で述べた通り Tate のアルゴリズムが用いられるわけであるが, 実はその途中で行われる代数構造（素イデアル分解等）の計算に膨大な時間を要する. 実際, OS Windows 7 32bit 版, Intel$^{\text{TM}}$ Core-i5 3.30GHz CPU と 4.00GB メモリを搭載した環境で MAGMA 上で計算を行った所, 丸一日（約 22 時間）程を要した. 将来的にはこのようなチェックを数多くの曲線に対して行う必要があるため, より効率的なアルゴリズムの開発, または現存のアルゴリズムの高速化が期待される.

このように至る所良い還元を持つ楕円曲線の例をたくさん作る為には, 代数体上の Mordell-Weil 群の計算が欠かせない. この方面の詳細については, 拙文 [6] および [7] に書いたのでこちらを参照されたい. 前者は “non-admissible” と呼ばれる特殊なケースに対しての計算限界について述べており, 後者は一般論の概説と, データベース構築に関する報告を行ったものとなっている. ベースとなった原論文 [5] および [8] も合わせて参照頂ければ幸いである. なお, これらを纏めた表は著者のウェブページ

`http://www2.math.kyushu-u.ac.jp/~s-yokoyama/ECtable.html`

にて公開・随時更新しているので, 興味のある方は参照頂きたい. なおデータの誤り等, 何かお気付きの点を見つけられた際には, ご連絡を頂ければ幸甚である.

5 楕円曲線に関する計算機的未解決問題

最後に楕円曲線の階数に関する興味深い予想を紹介する. これは講演終了後の質疑応答において白柳潔氏（東邦大学）よりご質問頂き, その際の説明を詳しく述べたものである. 話題を提供下さり, この場を借りて御礼申し上げたい.

予想 5.1. $\mathbb{Q}$ 上定義された楕円曲線で階数が幾らでも大きなものが存在するか？

ここで「階数」とは勿論 Mordell-Weil 群 $E(\mathbb{Q})$ の階数のことである. 階数を伸ばすと同時に, 互いに独立な無限位数の有理点をきちんと求める必要があるため, 非常に hard な問題である. 現時点（2011 年 12 月）における（モデル付きの）下限の世界記録は Noam Elkies（Harvard 大学）による 28 であり, 次のようなモデルで与えられる：

$$
\begin{aligned}
&y^2+xy+y=x^3-x^2\\
&-200677624155755265850332082093385427509302303121789565 02x\\
&+344816117950305564670329856903907203748559443593191 8\\
&\quad 0361266008296291939448732243429
\end{aligned}
$$

現時点で決定されている 28 個の互いに独立な生成元は次の通りである.

$$
\begin{aligned}
P_1 &= (-212415009125438107329213746 3, 259854492051899599030515511070780628911531)\\
P_2 &= (233450986603470175688475453 7, 188720041954944691808683165528036279 31531)\\
P_3 &= (-167173605406236906387903866 3, 251709377261144287808506947241319126049131)\\
P_4 &= (213913026013915666649298213 7, 366395091714397292024214596929412975 27531)\\
P_5 &= (153470676446712072388547733 7, 854295853460176942890210328627810727995 31)\\
P_6 &= (-273107948787567703334157506 3, 262521815484332191641284072623902143387531)\\
P_7 &= (277572626684457164970545853 7, 128457554740140602488694876990826403699 31)\\
P_8 &= (149438572932718895754183381 7, 884866055277334059861164945140492334114 51)\\
P_9 &= (186843822862088735850906525 7, 592374032144377087127251403930593585891 31)\\
P_{10} &= (200894510882574377486654253 7, 476906778801255528821517507815412447115 31)\\
P_{11} &= (234836054091802516965163293 7, 174929300062005578573403324764488043635 31)\\
P_{12} &= (-147208400709048117447000866 3, 246643450653503714199947441549759798469131)\\
P_{13} &= (292412860770806121336328893 7, 283502644314888785014883564747673758995 31)\\
P_{14} &= (537499389106606189329393453 7, 286188908427263386451175031916479893731531)\\
P_{15} &= (170969076823335452333400855 7, 718988349746860894661597005292159809216 31)\\
P_{16} &= (245095401135359314407259518 7, 444522817353263435704926255061071473653 1)\\
P_{17} &= (296925470927355916746467493 7, 327668930753662708013336825431604696875 31)\\
P_{18} &= (271191493494169260133288293 7, 206843661277838169865041398150659061353 1)\\
P_{19} &= (200785860779968545287783289 37, 277960854113780660465605172562462403009153 1)\\
P_{20} &= (215808245024073477431781069 7, 349943734019640268099696622418009012547 31)\\
P_{21} &= (200464545824705902240322493 7, 480493297807046455224398669998884754675 31)\\
P_{22} &= (297574945094799626494709133 7, 333989898260753223020893441010485786913 1)\\
P_{23} &= (-210249046768628515014734786 3, 259576391459875789571677393171687203227531)\\
P_{24} &= (311583179915063034902194537, 168104385229980603540109472915660153473931)\\
P_{25} &= (277393100834186523144377181 7, 126321628346499210024141162737692758134 51)\\
P_{26} &= (215658118814376840936346138 7, 351250929640229088970041505163751780873 31)\\
P_{27} &= (386633049987241250881565913 7, 121197755655944226293036926715025847322531)\\
P_{28} &= (223086828977357602377867873 7, 285587600305974856633870206007686400285 31)
\end{aligned}
$$

階数の下限	発見年	発見者
3	1938	Billing
4	1945	Wiman
6	1974	Penney - Pomerance
7	1975	Penney - Pomerance
8	1977	Grunewald - Zimmert
9	1977	Brumer - Kramer
12	1982	Mestre
14	1986	Mestre
15	1992	Mestre
17	1992	Nagao
19	1992	Fermigier
20	1993	Nagao
21	1994	Nagao - Kouya
22	1997	Fermigier
23	1998	Martin - McMillen
24	2000	Martin - McMillen
28	2006	Elkies

参考：rank$(E(\mathbb{Q}))$ の記録とその樹立年次

Elkies による構成が発表される前の世界記録は Martin - McMillen (2000) によるものであったが, これとは大きく違い, 独立な有理点の各成分が $\mathbb{Z}$ の元から得られている点は非常に興味深い. なお P_{29} が存在するかどうかは現在のところ知られていない.

やや反則技であるが, 上とは逆に楕円曲線を固定して基礎体を拡大していった場合はどうなるか？という予想も考えられる. こちらは既に木田雅成氏（電気通信大学）が構成法を見つけている：

定理 5.2 (Kida, 1993). $E: y^2 = x^3 - x$ ($\mathbb{Q}$ 上定義) とし,

$$K_m = \mathbb{Q}(\sqrt{q_1}, \sqrt{q_2}, \cdots, \sqrt{q_m})$$

とおく. ここに q_i は相異なる素数で mod 8 で 5 または 7 に合同なものとする. この時 m を大きくすると, rank(E, K_m) は幾らでも大きくなる.

謝辞

今回このように数式処理のカンファレンスにて講演の機会を頂き, また参加者の方々より貴重なアドバイスを数多く頂戴致しました. 皆様に感謝申し上げると共に, 本企画の代表者である高橋正先生（甲南大学）および副代表者である近藤祐史先生（香川高専）に厚く御礼申し上げます.

参考文献

[1] J. Cremona, *Algorithms for modular elliptic curves*, second edition, Cambridge University Press, Cambridge (1997).

[2] S. Siksek, *Infinite descent on elliptic curves*, Rocky Mountain J. Math. **25** (1995), no. 4, 1501-1538.

[3] J. H. Silverman, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. **55** (1990), no. 192, 723-743.

[4] D. Simon, *Computing the rank of elliptic curves over number fields*, LMS JCM vol. **5** (2002), 7-17.

[5] S. Yokoyama, *On elliptic curves with everywhere good reduction over certain number fields*, preprint (2011).

[6] 横山俊一, 二次体上至る所 good reduction を持つ楕円曲線について, 第 6 回福岡数論研究集会報告集 (2012).

[7] 横山俊一, 至る所良い還元を持つ楕円曲線について：計算機的手法とその最近の進展, 第 9 回「代数学と計算」研究集会（AC2011）報告集 (2012).

[8] S. Yokoyama and Y. Shimasaki, *Non-existence of elliptic curves with everywhere good reduction over some real quadratic fields*, J. Math-for-Industry, vol.**3** (2011B-4), 113-117.

Shun'ichi Yokoyama
Graduate School of Mathematics, Kyushu University
744 Motooka, Nishi-ku, Fukuoka, 819-0395, Japan
E-mail Address: s-yokoyama@math.kyushu-u.ac.jp

※ 所属は 2011 年度のものです.